

розпорядженні засоби збирання та аналізу даних про власну діяльність. За відсутності даних засобів навчальні заклади не будуть знати, що в їхній системі працює добре, а що потребує уваги, також невідомі результати нововведень. Інформаційні системи, що стосуються моніторингу якості, деякою мірою залежать від місцевих умов, але вони, принаймні, повинні охоплювати: навчальні та наукові досягнення студентів та показники їх успішності; попит на випускників на ринку праці; задоволеність студентів програмами підготовки за освітньо-кваліфікаційними рівнями «бакалавр», «магістр»; ефективність організації навчального процесу; склад студентів і його аналіз; професорсько-викладацький склад та його аналіз; доступні навчальні ресурси; головні показники освітньої діяльності даного навчального закладу.

Джерела:

1. Сергієнко В.П., Франчук В.М., Микитенко П.В. Використання інформаційно-комунікаційних технологій управління якістю освіти в педагогічному університеті. // Інформатика та інформаційні технології. - 2012. - №4. - С. 2 – 5.
2. Франчук В.М. Автоматизована система рейтингового оцінювання діяльності студентів і викладачів університету. IV International Summer School "Education Measurement: Teaching, Research, and Practice" is held under the support of the EU within the framework of the EU Project 145029-TEMPUS-2008-SE-JPCR "Educational Measurements Adapted to EU Standards".

Побудова захищеної системи реалізації транзакцій з використанням бібліотеки JcardSim

Гладкий Р.В, Желізняк Г.О.

Національний університет «Львівська політехніка», Львівський коледж Державного університету телекомунікацій, roman.gladkuy@gmail.com, zhelizniak_yosyf@ukr.net

In this article were analyzed ways to provide reliable and security solution, using smart-card based systems. As platform implementation has been used open source library JCardSim. Additionally, described open source used technologies, standards and specifications for communication with smart cards, methods to provide possibility of update and enhance mentioned solution.

Швидкий розвиток інтернету і безпроводних засобів цифрового зв'язку викликали великі зміни в способі використання електронної комерції. Із цим прогресом змінились також способи виконання дій, пов'язаних із покупкою товарів в інтернет магазинах, оплатою послуг. Виникла потреба у створенні систем безпеки для надійного використання електронної комерції. При розробці таких інформаційних систем є необхідність в реалізації безпеки та захисту даних, як на програмному, так і на фізичному рівні. Для захисту інформаційної системи на фізичному рівні ефективним інструментом є смарт-картки з вбудованим елементом безпеки, що надає доступ тільки

авторизованому користувачеві через протокол передачі даних. На відміну від захисту на програмному рівні, відсутня можливість будь-якої прямої взаємодії із програмою, зокрема пошук дефектів користувачем, через які можна оминати безпеку системи. Розробнику не обов'язково знати принципи роботи елемента безпеки чи протоколу передавання даних, для розробки програмного продукту достатньо мати загальні навички програмування та роботи із документацією.

Основною метою роботи є створення безпечної і захищеної системи, що дає змогу проводити транзакції із грошима за допомогою смарт-карток, а також терміналу для взаємодії із розробленим рішенням і підсистеми для автоматизованої валідації за допомогою тестових випадків. Можна виділити такі компоненти (див. рис.) розробленої системи 1)ужиток для смарт-картки із набором функціоналу для проведення транзакції; 2)термінал, для роботи із смарт-картками; 3)система для автоматичної валідації роботи ужитку за допомогою тестів; 4)емулятор смарт-картки для тестування і валідації роботи ужитку. Для реалізації завдання використано бібліотеку з відкритим вихідним кодом JCardSim (Java Card Runtime Enviroment Simulator) - методи і засоби для розробки Java Card застосунків і роботи із смарт-картками [1], а також документацію для смарт-карток, що описана в специфікаціях ISO-7816 [2], Open Card [3], Global Platform [4], та інших.

Аплет для смарт-картки є основною складовою частиною системи і містить набір функціоналів для захищених операцій: аутентифікації користувача, отримання приватної інформації, видачі валюти користувачеві та інші.

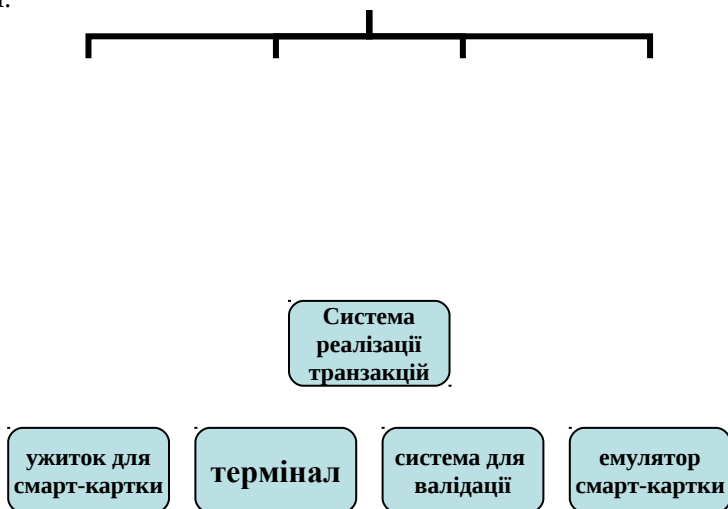


Рисунок. Структурна схема системи реалізації транзакцій

Термінал використовується для надання зручного інтерфейсу доступу до смарт-картки: надсилання запитів на проведення операцій та отримання і опрацювання відповідей. Взаємодія із картою відбувається через APDU команди (Application Protocol Data Unit – протокол що використовується для обміну даними із смарт-картками) [4]. Програмна складова що виконує валідацію, дозволяє виконувати завантаження тестів на розробленому аплеті, та аналізує результати їх виконання за критерієм відповідності параметрам безпеки. Це дозволяє проводити автоматизоване тестування в процесі розробки проміжних версій та відразу виправляти знайдені помилки. Емулятор смарт-картки виконує ті ж дії, що й чіп на картці. Використовується для прискорення завантаження тестів, а також для можливості розробки застосунків без використання апаратних пристроїв.

При користуванні системою можна виділити два основні потоки даних:

- запит користувача на транзакцію, тут користувач повинен надати необхідні дані в терміналі для авторизації чи виконання конкретної дії;
- результат виконання транзакції у вигляді повідомлення про її успішне завершення чи помилку.

Проведено експериментальні дослідження надійності даної системи, тестування та аналіз розробленого рішення. Приведено приклади тестових результатів та показана можливість подальшої оптимізації та оновлення системи.

Практична цінність розробленої системи полягає в можливості використання її як захищеної системи для операцій із валютою. А також передбачено можливості функціонального розширення, оновлення реалізації, покривання нового функціоналу додатковими тестами та автоматизованого тестування для забезпечення захищеності та надійності даної системи.

Джерела

1. Java Card Runtime Enviroment Simulator 2.2.2. - <https://jcardsim.org/>
2. ISO/IEC 7816, http://www.iso.org/iso/catalogue_detail.htm?csnumber=45989
3. OpenCard, <http://www.openscdp.org/>
4. GlobalPlatform, <http://www.globalplatform.org/>

Вільнопоширюване програмне забезпечення в контексті варіативності моделей комп'ютерно-орієнтованого середовища навчання предметів природничо-математичного циклу

Гриб'юк О.О., Хошаба О.М.

Інститут інформаційних технологій і засобів навчання НАПН України, Вінницький національний технічний університет, olenagrybyuk@gmail.com

Taking into account the specific technical characteristics of dissonance on computer equipment used in schools, in the design of the individual components of computer-